ABSTRACT OF THE DISCLOSURE

EFFICIENT METHOD FOR PROVIDING SECURE REMOTE ACCESS

A remote user, two-way authentication and password change protocol that also allows parties to optionally establish a session key which can be used to protect subsequent communication. In a preferred embodiment, a challenge token is generated and exchanged which is a one-time value that includes a random value that changes from session to session. The construction and use of the challenge token avoids transmission of the password or even the transmission of a digest of the password itself. Thus the challenge token does not reveal any information about a secret password or a digest of the password.